BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problem Mailbox.

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-344216
(43)Date of publication of application : 14.12.2001

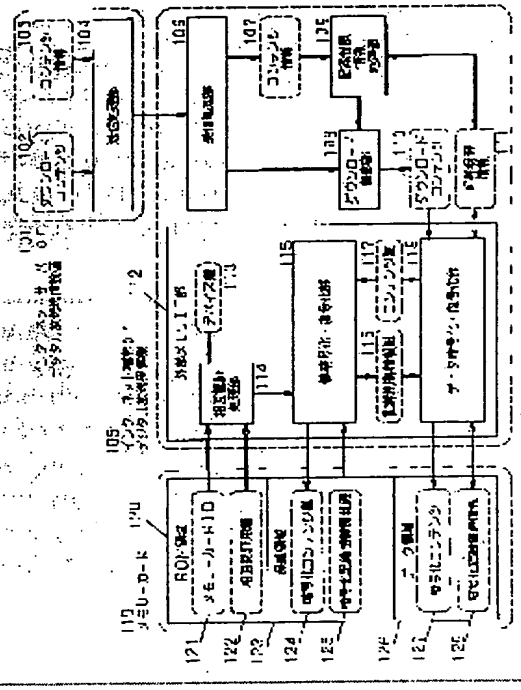
(51)Int.Cl. G06F 15/00
G06F 12/14
G06F 17/60
G06K 17/00
G06K 19/073
G06K 19/00

(21)Application number : 2000-167259
(22)Date of filing : 05.06.2000

(71)Applicant : MATSUSHITA ELECTRIC IND CO LTD
(72)Inventor : NAGAMIZU SADAAKI

(54) DOWNLOAD SYSTEM USING MEMORY CARD WITH RECORDING LIMIT INFORMATION

(57)Abstract:
PROBLEM TO BE SOLVED: To solve such a problem that a conventional download system can not update recording limit information recorded on a memory card without using a specific equipment.
SOLUTION: Since ciphered recording limit information is recorded in a data area of a memory card and a recording limit information key and a contents key are recorded in a protection area readable and writable after the success of mutual certification of the memory card, the contents of information can be downloaded in accordance with the recording limit information while preventing the recording limit information for preventing the generation of illegal download and charging download from being easily rewritten/read out, so that the recording limit information can be updated without requiring a specific equipment.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2001－344216
（P2001－344216A）
(43)公開日　平成13年12月14日(2001.12.14)

(51)Int.Cl.'		識別記号	FI		テーマコード(参考)
Ｇ０６Ｆ	15/00	３３０	Ｇ０６Ｆ 15/00	３３０Ｚ	５Ｂ０１７
	12/14	３２０	12/14	３２０Ｅ	５Ｂ０３５
	17/60	ＺＥＣ	17/60	ＺＥＣ	５Ｂ０４９
		３０２		３０２Ｅ	５Ｂ０５８
		５１０		５１０	５Ｂ０８５

審査請求　未請求　請求項の数６　ＯＬ　（全　８　頁）　最終頁に続く

(21)出願番号　特願2000－167259(P2000－167259)

(22)出願日　平成12年６月５日(2000.6.5)

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真1006番地

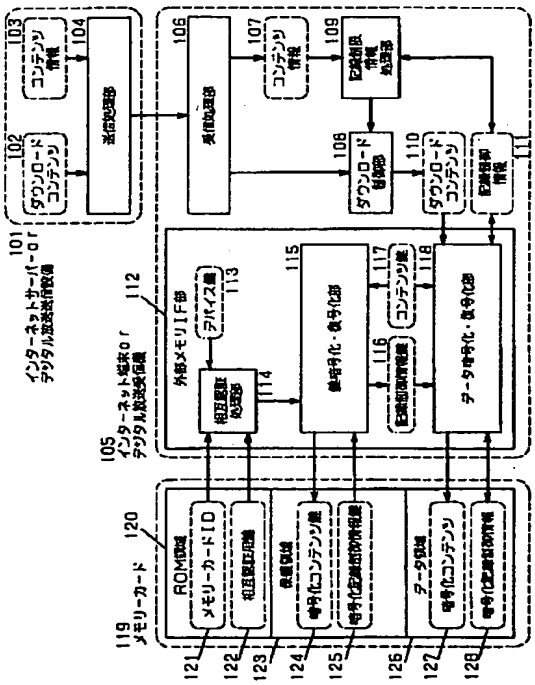
(72)発明者　長水　禎明
大阪府門真市大字門真1006番地　松下電器産業株式会社内

(74)代理人　100097445
弁理士　岩橋　文雄　（外２名）

最終頁に続く

(54)【発明の名称】　記録制限情報付メモリーカードを用いたダウンロードシステム

(57)【要約】
【課題】　従来のダウンロードシステムは、メモリーカードに記録された記録制限情報が特殊な機器を用いなければ更新できないという課題があった。
【解決手段】　メモリーカードのデータ領域に暗号化記録制限情報を、メモリーカードの相互認証成功後に読み書きできる保護領域に記録制限情報鍵、および、コンテンツ鍵を記録させておくことで、従来通り不正なダウンロードの防止、ダウンロードに対する課金を実現するための記録制限情報を、安易に書き換え、読み出しできないようにしながら、記録制限情報に従ったコンテンツのダウンロードが実現でき、特殊な機器を用いなくても記録制限情報の更新が実現できようにする。



1

【特許請求の範囲】

【請求項１】　ダウンロードコンテンツとそのコンテンツ情報を送信する送信処理部を有するインターネットサーバーやデジタル放送送信設備と、前記ダウンロードコンテンツとそのコンテンツ情報を受信する受信処理部、接続されたメモリーカードと相互認証を行う相互認証処理部、鍵の暗号化・復号化を行う鍵暗号化・復号化部、データの暗号化・復号化を行うデータ暗号化・復号化部、メモリーカードに記録された記録制限情報と受信したコンテンツ情報を比較処理する記録制限情報処理部、前記記録制限情報処理部の処理結果に応じてコンテンツのダウンロードを制御するダウンロード制御部を有するデジタル放送受信機やインターネット端末と、読み出しのみ可能なROM領域、相互認証成功時に読み書きできる保護領域、相互認証結果に関係なく読み書きできるデータ領域を有するメモリーカードから成る、ダウンロードシステムにおいて、接続されたメモリーカードの相互認証成功後、保護領域から暗号化記録制限情報鍵を読み出し、相互認証部からの情報を用いて復号化し、得られた記録制限情報鍵を用いて、データ領域から読み出した暗号化記録制限情報を復号化し、得られた記録制限情報と受信したコンテンツ情報と比較することで、接続したメモリーカードに対してコンテンツをダウンロードできるかどうかを制御することを特長とした、ダウンロードシステム。

【請求項２】　コンテンツのダウンロード完了後、そのコンテンツ情報に基づき、記録制限情報を更新し、記録制限情報鍵を用いて暗号化し、得られた暗号化記録制限情報をメモリーカードのデータ領域に書き込み、相互認証部からの情報を用いて記録制限情報鍵を暗号化し、得られた暗号化記録制限情報鍵をメモリーカードの保護領域に書き込むことを特長とした、請求項1記載のダウンロードシステム。

【請求項３】　記録制限情報として、ダウンロード可能なデジタル放送やインターネットのコンテンツ配信業者に関する情報を用いることを特長とした、請求項1、および、請求項2記載のダウンロードシステム。

【請求項４】　記録制限情報として、ダウンロード可能なコンテンツの種類に関する情報を用いることを特長とした、請求項1、および、請求項2記載のダウンロードシステム。

【請求項５】　記録制限情報として、ダウンロード可能なコンテンツの残数や残り容量に関する情報を用いることを特長とした、請求項1、および、請求項2記載のダウンロードシステム。

【請求項６】　記録制限情報として、ダウンロード可能な期間に関する情報を用いることを特長とした、請求項1、および、請求項2記載のダウンロードシステム。

【発明の詳細な説明】

【０００１】

2

【発明の属する技術分野】本発明は、記録制限情報付メモリーカードを用いたダウンロードシステムに関する。

【０００２】

【従来の技術】図2は、ROM領域に暗号化記録制限情報を記録したメモリーカードを用いたダウンロードシステムのブロック図である。図2において、201はインターネットサーバーやデジタル放送送信設備、202はダウンロードコンテンツ、203はコンテンツ情報、204は送信処理部、205はインターネット端末やデジタル放送受信機、206は受信処理部、207はコンテンツ情報、209は記録制限情報処理部、208はダウンロード制御部、210はダウンロードコンテンツ、211は記録制限情報、212は外部メモリIF部、213は記録制限情報鍵、214は記録制限情報復号化部、215はコンテンツ鍵、216はデータ暗号化･復号化部、217はメモリーカード、218はROM領域、219は暗号化記録制限情報、220はデータ領域、221は暗号化コンテンツである。上記従来例において、メモリーカードに記録された記録制限情報に基づく、コンテンツのダウンロード動作について説明する。不正なダウンロードの防止、ダウンロードに対する課金を実現するための記録制限情報は、安易に書き換え、読み出しできないようメモリーカード217のROM領域218に、記録制限情報鍵213で暗号化されて記録されている。インターネット端末やデジタル放送受信機205は、接続されたメモリーカード217のROM領域218から暗号化記録制限情報219を読み出し、機器内部の記録制限情報鍵213を用いて記録制限情報復号化部214で復号化し、得られた記録制限情報211は記録制限情報処理部209に送られる。一方、受信処理部206は、インターネットサーバーやデジタル放送送信設備201の送信処理部204より送信されるコンテンツ情報203を受信し、記録制限情報処理部209に送る。記録制限情報処理部209では、これら記録制限情報211とコンテンツ情報207とを比較して、ダウンロード可能かどうかの情報をダウンロード制御部208に送る。ダウンロード可能であればダウンロード制御部208はコンテンツ202をダウンロードし、機器内部のコンテンツ鍵215を用いてデータ暗号化･復号化部216で暗号化し、得られた暗号化コンテンツをメモリーカード217のデータ領域220に暗号化コンテンツ221として書き込む。従って、上記従来のダウンロードシステムおいては、メモリーカードのROM領域に記録制限情報が記録されているため、特殊な機器を用いなければ記録制限情報を更新することができなかった。また、暗号化記録制限情報を復号化する記録制限情報鍵、コンテンツを暗号化するコンテンツ鍵は、インターネット端末やデジタル放送受信機の内部に記録しておかなければならないので、異なる記録制限情報鍵、コンテンツ鍵を持つ他の機器では、記録制限情報が復号化できなかったり、他の機器でダウンロードしたコンテンツを読み出すことができなかった。

【０００３】

【発明が解決しようとする課題】このため、上記従来のダウンロードシステムは、メモリーカードに記録された記録制限情報が特殊な機器を用いなければ更新できないという問題と、異なる記録制限情報鍵、コンテンツ鍵を持つ他のインターネット端末やデジタル放送受信機では、記録制限情報が復号化できなかったり、他の機器でダウンロードしたコンテンツを読み出すことができないという問題を有していた。本発明は、上記の問題を解決するもので、メモリーカードのデータ領域に暗号化記録制限情報を、メモリーカードの相互認証成功後に読み書きできる保護領域に記録制限情報鍵、および、コンテンツ鍵を記録させておくことで、従来通り不正なダウンロードの防止、ダウンロードに対する課金を実現するための記録制限情報を、安易に書き換え、読み出しできないようにしながら、記録制限情報に従ったコンテンツのダウンロードが実現でき、特殊な機器を用いなくても記録制限情報の更新が実現でき、さらに、他の機器でも記録制限情報の復号化、および、ダウンロードしたコンテンツの読み出しが実現でき、また、ダウンロード結果に従い、記録制限情報を更新してメモリーカードに書き込むことが実現できる、ダウンロードシステムを提供することを目的とする。

【０００４】

【課題を解決するための手段】上記問題を解決するために本発明は、メモリーカードのメモリーカードIDと相互認証用鍵、インターネット端末やデジタル放送受信機内部のデバイス鍵を用いてそのメモリーカードの相互認証を行う手段と、相互認証結果によりメモリーカードの保護領域から読み出した暗号化記録制限情報鍵を復号化する手段と、記録制限情報鍵を用いてメモリーカードのデータ領域から読み出した暗号化記録制限情報を復号化する手段と、復号化した記録制限情報と受信したコンテンツ情報を比較処理する手段と、比較結果によりダウンロードを制御する手段と、ダウンロード後にコンテンツ情報に従い記録制限情報を更新する手段と、更新した記録制限情報を記録制限情報鍵を用いて暗号化してメモリーカードのデータ領域に記録する手段と、記録制限情報鍵を暗号化してメモリーカードの保護領域に記録する手段と、相互認証結果によりコンテンツ鍵を暗号化してメモリーカードの保護領域に記録する手段を有することを特長とする。以上により、記録制限情報に従ったコンテンツのダウンロードが実現でき、特殊な機器を用いなくても記録制限情報の更新が実現でき、さらに、他の機器でも記録制限情報の復号化、および、ダウンロードしたコンテンツの読み出しが実現でき、また、ダウンロード結果に従い、記録制限情報を更新してメモリーカードに書き込むことが実現できる。

【０００５】

【発明の実施の形態】本発明の請求項1に記載の発明は、メモリーカードのメモリーカードIDと相互認証用

鍵、インターネット端末やデジタル放送受信機内部のデバイス鍵を用いてそのメモリーカードの相互認証を行う手段と、相互認証結果によりメモリーカードの保護領域から読み出した暗号化記録制限情報鍵を復号化する手段と、記録制限情報鍵を用いてメモリーカードのデータ領域から読み出した暗号化記録制限情報を復号化する手段と、復号化した記録制限情報と受信したコンテンツ情報を比較処理する手段と、比較結果によりダウンロードを制御する手段を有するものであり、記録制限情報に従ったコンテンツのダウンロードが実現できる作用を有する。また、請求項2に記載の発明は、上記の手段に加え、ダウンロード後にコンテンツ情報に従い記録制限情報を更新する手段と、更新した記録制限情報を記録制限情報鍵を用いて暗号化してメモリーカードのデータ領域に記録する手段と、記録制限情報鍵を暗号化してメモリーカードの保護領域に記録する手段と、相互認証結果によりコンテンツ鍵を暗号化してメモリーカードの保護領域に記録する手段を有するものであり、特殊な機器を用いなくても記録制限情報の更新が実現でき、さらに、他の機器でも記録制限情報の復号化、および、ダウンロードしたコンテンツの読み出しが実現できる作用を有する。また、請求項3に記載の発明は、上記の手段に加え、記録制限情報として、ダウンロード可能なデジタル放送やインターネットのコンテンツ配信業者に関する情報を比較する手段を有するものであり、記録されたコンテンツ配信業者からだけコンテンツのダウンロードできる作用を有する。また、請求項4に記載の発明は、上記の手段に加え、記録制限情報として、ダウンロード可能なコンテンツの種類に関する情報を比較する手段を有するものであり、記録された種類のコンテンツだけをダウンロードできる作用を有する。また、請求項5に記載の発明は、上記の手段に加え、記録制限情報として、ダウンロード可能なコンテンツの残数や残り容量に関する情報を比較する手段を有するものであり、記録された残数や残り容量を越えない分のコンテンツをダウンロードできる作用を有する。また、請求項6に記載の発明は、上記の手段に加え、記録制限情報として、ダウンロード可能な期間に関する情報を比較する手段を有するものであり、記録された期間だけコンテンツをダウンロードできる作用を有する。以下、本発明の実施の形態について、図1を用いて説明する。

（実施の形態1）図1は、本発明の実施の形態1におけるダウンロードシステムのブロック図である。本発明の実施の形態1における、メモリーカードに記録されたダウンロード可能なコンテンツ配信業者に関する記録制限情報に基づく、インターネット端末やデジタル放送受信機のコンテンツのダウンロード動作について、図1を用いて説明する。不正なダウンロードの防止、ダウンロードに対する課金を実現するための記録制限情報として、ダウンロード可能なコンテンツ配信業者に関する情報が、

5

安易に書き換え、読み出しできないよう、相互認証成功後に読み書きできるメモリーカード119の保護領域123に記録された記録制限情報鍵116で暗号化されて、相互認証結果に関係なく読み書きできるデータ領域126に暗号化記録制限情報128として記録されている。インターネット端末やデジタル放送受信機105は、接続されたメモリーカード119のROM領域120のメモリーカードID121と相互認証用鍵122、内部のデバイス鍵113を用いて相互認証処理部114でそのメモリーカードの相互認証を行う。鍵暗号化・復号化部115は、相互認証部114からの情報を用いて、メモリーカード119の保護領域123から読み出した暗号化記録制限情報鍵125を復号化し、記録制限情報鍵116を得る。データ暗号化･復号化部118は、得られた記録制限情報鍵116を用いて、メモリーカード119のデータ領域126より読み出した暗号化記録制限情報128を復号化し、記録制限情報111を得、記録制限情報処理部109に送られる。一方、受信処理部106は、インターネットサーバーやデジタル放送送信設備101の送信処理部104より送信されるコンテンツ配信業者に関する情報を含むコンテンツ情報103を受信し、記録制限情報処理部109に送る。記録制限情報処理部109では、コンテンツ情報107のコンテンツ配信業者に関する情報が、記録制限情報111のダウンロード可能なコンテンツ配信業者に関する情報に含まれているかどうか判断し、含まれていればダウンロード可能の情報をダウンロード制御部108に送る。ダウンロード可能であればダウンロード制御部108はコンテンツ102をダウンロードし、コンテンツ鍵117を用いてデータ暗号化･復号化部118で暗号化し、得られた暗号化コンテンツ127をメモリーカード119のデータ領域126に書き込む。さらに、コンテンツ鍵117は鍵暗号化･復号化部115で暗号化し、得られた暗号化コンテンツ鍵124をメモリーカード119の保護領域123に書き込む。以上のように本発明の実施の形態によれば、前記インターネットサーバーやデジタル放送送信設備101内部に、ダウンロードコンテンツ102とコンテンツ情報103を送信する送信処理部104を設け、前記インターネット端末やデジタル放送受信機105内部に、受信処理部106、記録制限情報処理部109、ダウンロード制御部108、相互認証処理部114、鍵暗号化･復号化部115、データ暗号化･復号化部118を設け、メモリーカード119内部に、ROM領域120、保護領域123、データ領域126を設けることにより、記録制限情報に従ったコンテンツのダウンロードが実現でき、特殊な機器を用いなくても記録制限情報の更新が実現でき、さらに、他の機器でも記録制限情報の復号化、および、ダウンロードしたコンテンツの読み出しが実現することができる。

（実施の形態2）図1は、本発明の実施の形態2におけるダウンロードシステムのブロック図である。本発明の実施の形態2における、メモリーカードに記録されたダウンロード可能なコンテンツの種類に関する記録制限情報

6

に基づく、インターネット端末やデジタル放送受信機のコンテンツのダウンロード動作について、図1を用いて説明する。不正なダウンロードの防止、ダウンロードに対する課金を実現するための記録制限情報として、ダウンロード可能なコンテンツの種類に関する情報が、安易に書き換え、読み出しできないよう、相互認証成功後に読み書きできるメモリーカード119の保護領域123に記録された記録制限情報鍵116で暗号化されて、相互認証結果に関係なく読み書きできるデータ領域126に暗号化記録制限情報128として記録されている。インターネット端末やデジタル放送受信機105は、接続されたメモリーカード119のROM領域120のメモリーカードID121と相互認証用鍵122、内部のデバイス鍵113を用いて相互認証処理部114でそのメモリーカードの相互認証を行う。鍵暗号化・復号化部115は、相互認証部114からの情報を用いて、メモリーカード119の保護領域123から読み出した暗号化記録制限情報鍵125を復号化し、記録制限情報鍵116を得る。データ暗号化･復号化部118は、得られた記録制限情報鍵116を用いて、メモリーカード119のデータ領域126より読み出した暗号化記録制限情報128を復号化し、記録制限情報111を得、記録制限情報処理部109に送られる。一方、受信処理部106は、インターネットサーバーやデジタル放送送信設備101の送信処理部104より送信されるコンテンツの種類に関する情報を含むコンテンツ情報103を受信し、記録制限情報処理部109に送る。記録制限情報処理部109では、コンテンツ情報107のコンテンツの種類に関する情報が、記録制限情報111のダウンロード可能なコンテンツの種類に関する情報に含まれているかどうか判断し、含まれていればダウンロード可能の情報をダウンロード制御部108に送る。ダウンロード可能であればダウンロード制御部108はコンテンツ102をダウンロードし、コンテンツ鍵117を用いてデータ暗号化･復号化部118で暗号化し、得られた暗号化コンテンツ127をメモリーカード119のデータ領域126に書き込む。さらに、コンテンツ鍵117は鍵暗号化･復号化部115で暗号化し、得られた暗号化コンテンツ鍵124をメモリーカード119の保護領域123に書き込む。以上のように本発明の実施の形態によれば、前記インターネットサーバーやデジタル放送送信設備101内部に、ダウンロードコンテンツ102とコンテンツ情報103を送信する送信処理部104を設け、前記インターネット端末やデジタル放送受信機105内部に、受信処理部106、記録制限情報処理部109、ダウンロード制御部108、相互認証処理部114、鍵暗号化･復号化部115、データ暗号化･復号化部118を設け、メモリーカード119内部に、ROM領域120、保護領域123、データ領域126を設けることにより、記録制限情報に従ったコンテンツのダウンロードが実現でき、特殊な機器を用いなくても記録制限情報の更新が実現でき、さらに、他の機器でも記録制限情報の復号化、および、ダウンロードしたコンテンツの読み出しが実現することができる。

7

（実施の形態3）図1は、本発明の実施の形態1におけるダウンロードシステムのブロック図である。本発明の実施の形態1における、メモリーカードに記録されたダウンロード可能なコンテンツの残数や残り容量に関する記録制限情報に基づく、インターネット端末やデジタル放送受信機のコンテンツのダウンロード動作について、図1を用いて説明する。不正なダウンロードの防止、ダウンロードに対する課金を実現するための記録制限情報として、ダウンロード可能なコンテンツ配信業者に関する情報が、安易に書き換え、読み出しできないよう、相互認証成功後に読み書きできるメモリーカード119の保護領域123に記録された記録制限情報鍵116で暗号化されて、相互認証結果に関係なく読み書きできるデータ領域126に暗号化記録制限情報128として記録されている。インターネット端末やデジタル放送受信機105は、接続されたメモリーカード119のROM領域120のメモリーカードID121と相互認証用鍵122、内部のデバイス鍵113を用いて相互認証処理部114でそのメモリーカードの相互認証を行う。鍵暗号化・復号化部115は、相互認証部114からの情報を用いて、メモリーカード119の保護領域123から読み出した暗号化記録制限情報鍵125を復号化し、記録制限情報鍵116を得る。データ暗号化･復号化部118は、得られた記録制限情報鍵116を用いて、メモリーカード119のデータ領域126より読み出した暗号化記録制限情報128を復号化し、記録制限情報111を得、記録制限情報処理部109に送られる。一方、受信処理部106は、インターネットサーバーやデジタル放送送信設備101の送信処理部104より送信されるコンテンツの数や容量に関する情報を含むコンテンツ情報103を受信し、記録制限情報処理部109に送る。記録制限情報処理部109では、コンテンツ情報107のコンテンツの数や容量に関する情報が、記録制限情報111のダウンロード可能なコンテンツの残数や残り容量に関する情報と比較し、数や容量をオーバーしなければダウンロード可能の情報をダウンロード制御部108に送る。ダウンロード可能であればダウンロード制御部108はコンテンツ102をダウンロードし、コンテンツ鍵117を用いてデータ暗号化･復号化部118で暗号化し、得られた暗号化コンテンツ127をメモリーカード119のデータ領域126に書き込む。さらに、コンテンツ鍵117は鍵暗号化･復号化部115で暗号化し、得られた暗号化コンテンツ鍵124をメモリーカード119の保護領域123に書き込む。また、ダウンロード完了後に、記録制限情報処理部109は、記録制限情報111のダウンロード可能なコンテンツの残数や残り容量を、ダウンロードした分だけ減少する。更新された記録制限情報111は、記録制限情報鍵116を用いてデータ暗号化･復号化部118で暗号化し、得られた暗号化記録制限情報128をメモリーカードのデータ領域126に書き込む。以上のように本発明の実施の形態によれば、前記インターネットサーバーやデジタル放送送信設備101内部に、ダウンロードコンテンツ102とコンテンツ情報103を送信する送信処理部104を設け、前記インターネット端末やデジタル放送受信機105内部に、受信処理部106、記録制限情報処理部109、ダウンロード制御部108、相互認証処理部114、鍵暗号化･復号化部115、データ暗号化･復号化部118を設け、メモリーカード119内部に、ROM領域120、保護領域123、データ領域126を設けることにより、記録制限情報に従ったコンテンツのダウンロードが実現でき、特殊な機器を用いなくても記録制限情報の更新が実現でき、さらに、他の機器でも記録制限情報の復号化、および、ダウンロードしたコンテンツの読み出しが実現でき、また、ダウンロード結果に従い、記録制限情報を更新してメモリーカードに書き込むことが実現できる。

8

（実施の形態4）図1は、本発明の実施の形態1におけるダウンロードシステムのブロック図である。本発明の実施の形態1における、メモリーカードに記録されたダウンロード可能な期間に関する記録制限情報に基づく、インターネット端末やデジタル放送受信機のコンテンツのダウンロード動作について、図1を用いて説明する。不正なダウンロードの防止、ダウンロードに対する課金を実現するための記録制限情報として、ダウンロード可能な期間に関する情報が、安易に書き換え、読み出しできないよう、相互認証成功後に読み書きできるメモリーカード119の保護領域123に記録された記録制限情報鍵116で暗号化されて、相互認証結果に関係なく読み書きできるデータ領域126に暗号化記録制限情報128として記録されている。インターネット端末やデジタル放送受信機105は、接続されたメモリーカード119のROM領域120のメモリーカードID121と相互認証用鍵122、内部のデバイス鍵113を用いて相互認証処理部114でそのメモリーカードの相互認証を行う。鍵暗号化・復号化部115は、相互認証部114からの情報を用いて、メモリーカード119の保護領域123から読み出した暗号化記録制限情報鍵125を復号化し、記録制限情報鍵116を得る。データ暗号化･復号化部118は、得られた記録制限情報鍵116を用いて、メモリーカード119のデータ領域126より読み出した暗号化記録制限情報128を復号化し、記録制限情報111を得、記録制限情報処理部109に送られる。一方、受信処理部106は、インターネットサーバーやデジタル放送送信設備101の送信処理部104より送信される現在時刻に関する情報を含むコンテンツ情報103を受信し、記録制限情報処理部109に送る。記録制限情報処理部109では、コンテンツ情報107の現在時刻に関する情報と、記録制限情報111のダウンロード可能な期間に関する情報と比較し、現在時刻が期間内に含まれていればダウンロード可能の情報をダウンロード制御部108に送る。ダウンロード可能であればダウンロード制御部108はコンテンツ102をダウンロードし、コンテンツ鍵117を用いてデータ暗号化･復号化部118で暗号化し、得られた暗号化コンテンツ127をメモリーカード119のデータ領域126に書き込む。さらに、コンテ

ンツ鍵117は鍵暗号化･復号化部115で暗号化し、得られた暗号化コンテンツ鍵124をメモリーカード119の保護領域123に書き込む。以上のように本発明の実施の形態によれば、前記インターネットサーバーやデジタル放送送信設備101内部に、ダウンロードコンテンツ102とコンテンツ情報103を送信する送信処理部104を設け、前記インターネット端末やデジタル放送受信機105内部に、受信処理部106、記録制限情報処理部109、ダウンロード制御部108、相互認証処理部114、鍵暗号化･復号化部115、データ暗号化･復号化部118を設け、メモリーカード119内部に、ROM領域120、保護領域123、データ領域126を設けることにより、記録制限情報に従ったコンテンツのダウンロードが実現でき、特殊な機器を用いなくても記録制限情報の更新が実現でき、さらに、他の機器でも記録制限情報の復号化、および、ダウンロードしたコンテンツの読み出しが実現することができる。

【０００６】

【発明の効果】以上のように本発明は、メモリーカードのメモリーカードIDと相互認証用鍵、インターネット端末やデジタル放送受信機内部のデバイス鍵を用いてそのメモリーカードの相互認証を行う手段と、相互認証結果によりメモリーカードの保護領域から読み出した暗号化記録制限情報鍵を復号化する手段と、記録制限情報鍵を用いてメモリーカードのデータ領域から読み出した暗号化記録制限情報を復号化する手段と、復号化した記録制限情報と受信したコンテンツ情報を比較処理する手段と、比較結果によりダウンロードを制御する手段を設けることにより、記録制限情報に従ったコンテンツのダウンロードが実現できる効果が得られる。また、上記の手段に加え、ダウンロード後にコンテンツ情報に従い記録制限情報を更新する手段と、更新した記録制限情報を記録制限情報鍵を用いて暗号化してメモリーカードのデータ領域に記録する手段と、記録制限情報鍵を暗号化してメモリーカードの保護領域に記録する手段と、相互認証結果によりコンテンツ鍵を暗号化してメモリーカードの保護領域に記録する手段を設けることにより、特殊な機器を用いなくても記録制限情報の更新が実現でき、さらに、他の機器でも記録制限情報の復号化、および、ダウンロードしたコンテンツの読み出しが実現できる効果が得られる。また、上記の手段に加え、記録制限情報として、ダウンロード可能なデジタル放送やインターネットのコンテンツ配信業者に関する情報を比較する手段を設けることにより、記録されたコンテンツ配信業者からだけコンテンツのダウンロードできる効果が得られる。また、上記の手段に加え、記録制限情報として、ダウンロード可能なコンテンツの種類に関する情報を比較する手段を設けることにより、記録された種類のコンテンツだけをダウンロードできる効果が得られる。また、上記の手段に加え、記録制限情報として、ダウンロード可能なコンテンツの残数や残り容量に関する情報を比較する手段を設けることにより、記録された残数や残り容量を越えない分のコンテンツをダウンロードできる効果が得られる。また、上記の手段に加え、記録制限情報として、ダウンロード可能な期間に関する情報を比較する手段を設けることにより、記録された期間だけコンテンツをダウンロードできる効果が得られる。

【図面の簡単な説明】

【図１】本発明の実施の形態1、2、3、4における記録制限情報付きメモリーカードを用いたダウンロードシステムのブロック図

【図２】従来の記録制限情報付きメモリーカードを用いたダウンロードシステムのブロック図

【符号の説明】

１０１　インターネットサーバーやデジタル放送送信設備
１０２　ダウンロードコンテンツ
１０３　コンテンツ情報
１０４　送信処理部
１０５　インターネット端末やデジタル放送受信機
１０６　受信処理部
１０７　コンテンツ情報
１０８　ダウンロード制御部
１０９　記録制限情報処理部
１１０　ダウンロードコンテンツ
１１１　記録制限情報
１１２　外部メモリIF部
１１３　デバイス鍵
１１４　相互認証処理部
１１５　鍵暗号化･復号化部
１１６　記録制限情報鍵
１１７　コンテンツ鍵
１１８　データ暗号化･復号化部
１１９　メモリーカード
１２０　ROM領域
１２１　メモリーカードID
１２２　相互認証用鍵
１２３　保護領域
１２４　暗号化コンテンツ鍵
１２５　暗号化記録制限情報鍵
１２６　データ領域
１２７　暗号化コンテンツ
１２８　暗号化記録制限情報
２０１　インターネットサーバーやデジタル放送送信設備
２０２　ダウンロードコンテンツ
２０３　コンテンツ情報
２０４　送信処理部
２０５　インターネット端末やデジタル放送受信機
２０６　受信処理部
２０７　コンテンツ情報

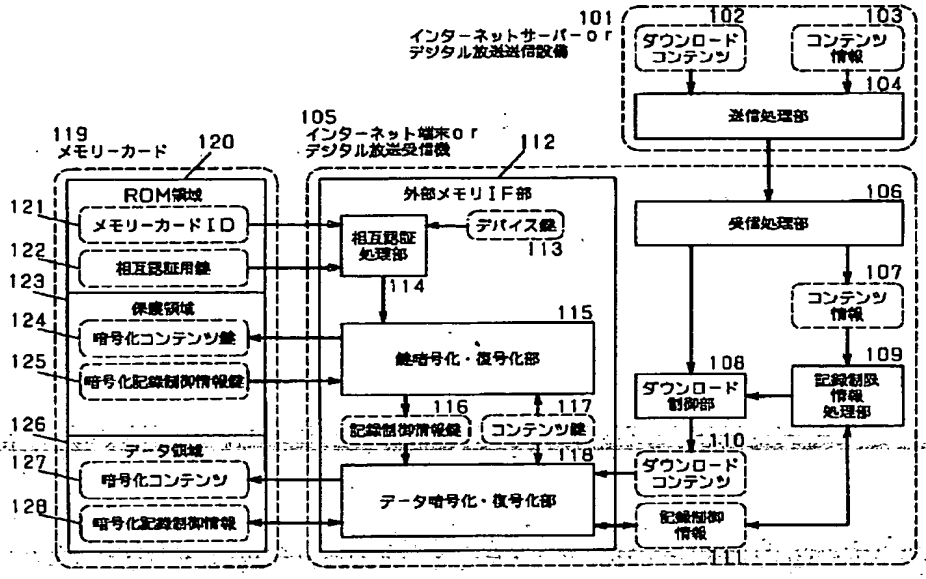
11

２０８　ダウンロード制御部
２０９　記録制限情報処理部
２１０　ダウンロードコンテンツ
２１１　記録制限情報
２１２　外部メモリIF部
２１３　記録制限情報鍵
２１４　記録制限情報復号化部

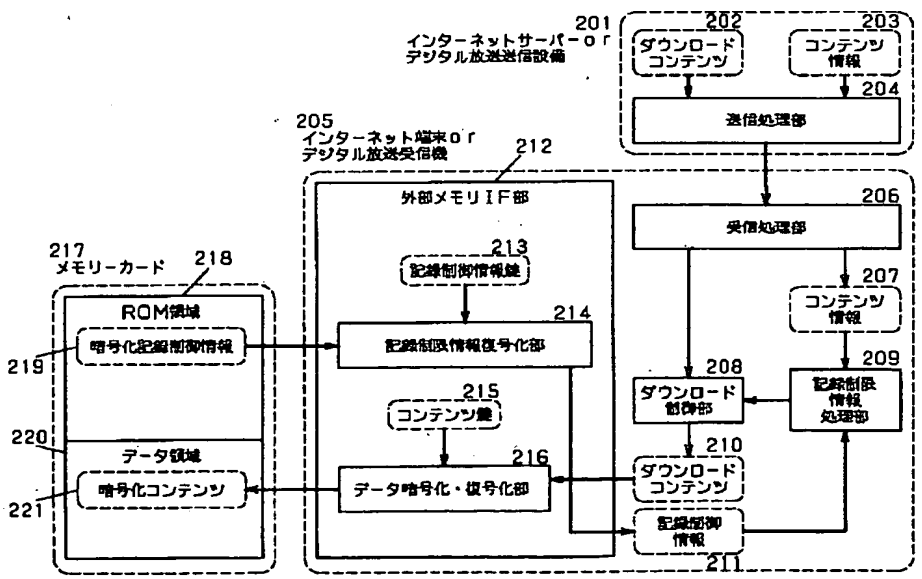
12

＊２１５　コンテンツ鍵
２１６　データ暗号化･復号化部
２１７　メモリーカード
２１８　ROM領域
２１９　暗号化記録制限情報
２２０　データ領域
＊　２２１　暗号化コンテンツ

【図１】



【図２】



フロントページの続き

(51) Int. Cl.[7]		識別記号	FI		テーマコード（参考）
Ｇ０６Ｆ	17/60	５１２	Ｇ０６Ｆ	17/60	５１２
Ｇ０６Ｋ	17/00		Ｇ０６Ｋ	17/00	Ｌ
	19/073			19/00	Ｐ
	19/00				Ｑ

Ｆターム（参考） 5B017 AA06 BA07 CA16
5B035 BB09 BC00 CA11 CA38
5B049 AA05 BB11 CC05 CC36 DD01
DD04 EE01 EE23 EE28 FF03
FF04 FF08 GG04 GG07 GG10
5B058 CA23 KA08 KA31 YA20
5B085 AE09 AE12 AE13 BG07